

UNITED STATES DISTRICT COURT

for the
Central District of California

In the Matter of the Search of)
(Briefly describe the property to be searched or identify the)
person by name and address))

Case No. **2:22-MJ-03847**

A Black / grey Samsung cell phone with a black /)
silver phone case the ("SUBJECT DEVICE"))
)
)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment A

located in the Central District of California, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. §§ 922 (g) (1), (9)

Offense Description
Felon and Domestic Violence Misdemeanant in Possession of a Firearm and Ammunition

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/

Applicant's signature

Brandice A. Olmos, SA ATF

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: _____

Judge's signature

City and state: Los Angeles, CA

Honorable Rozella A. Olive, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

PROPERTY TO BE SEARCHED

The following digital device (the "SUBJECT DEVICE"), seized on August 21, 2022, and currently maintained in the custody of Burbank Police Department ("BPD"), in Burbank, California:

1. Black/grey Samsung cell phone with a black/silver phone case (the "SUBJECT DEVICE").

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 922(g)(1), (9) (Felon and Domestic Violence Misdemeanant in Possession of a Firearm and Ammunition) the "Subject Offense"), namely:

a. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

b. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital device and which relate to the above-named violations;

c. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

d. Records, documents, programs, applications, materials, or conversations relating to the sale or purchase of

guns or ammunition, including correspondence, receipts, records, and documents noting prices or times when guns or ammunition were bought, sold, or otherwise distributed;

e. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of guns or ammunition;

f. Contents of any calendar or date book;

g. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

h. Any SUBJECT DEVICE which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense, and forensic copies thereof.

i. With respect to any SUBJECT DEVICE containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- iii. evidence of the attachment of other devices;
- iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;
- v. evidence of the times the device was used;
- vi. passwords, encryption keys, and other access devices that may be necessary to access the device;
- vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;
- viii. records of or information about Internet Protocol addresses used by the device;
- ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

II. SEARCH PROCEDURE FOR DIGITAL DEVICE(S)

3. In searching the SUBJECT DEVICE (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any SUBJECT DEVICE capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search the SUBJECT DEVICE where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the SUBJECT DEVICE as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search the digital device beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in the SUBJECT DEVICE capable of containing any of the items to be seized to the search protocols to determine whether the SUBJECT DEVICE and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

f. If the search determines that the SUBJECT DEVICE does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the SUBJECT DEVICE and delete or destroy all forensic copies thereof.

g. If the search determines that the SUBJECT DEVICE does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the SUBJECT DEVICE is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain the SUBJECT DEVICE if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the SUBJECT DEVICE, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

4. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

5. During the execution of this search warrant, law enforcement is permitted to (1) depress RUIZ's thumb- and/or fingers onto the fingerprint sensor of the SUBJECT DEVICE (only if the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of RUIZ's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in

order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Brandice A. Olmos, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of an application for a warrant to search the following digital device (the "SUBJECT DEVICE"), seized on or about August 21, 2022, by the Burbank Police Department ("BPD"), and currently in BPD custody in Burbank, California, as described more fully in Attachment A:

a. a black/grey Samsung cell phone with a black/silver phone case (the "SUBJECT DEVICE").

2. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 922(g)(1), (9) (Felon and Domestic Violence Misdemeanant in Possession of a Firearm and Ammunition) (the "Subject Offense"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrant and does not purport to set forth all my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this

affidavit are related in substance and in part only, all dates and times are on or about those stated.

II. BACKGROUND OF AFFIANT

4. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms, and Explosives ("ATF"), United States Department of Justice, and have been so employed since August 2021. Prior to being employed as an ATF Special Agent, I was a student intern for the United States Marshals Service for approximately one year.

5. I graduated from Eastern Michigan University with a Bachelor of Arts degree in Criminology, while receiving a full athletic and academic scholarship. I also graduated from California Baptist University with a Master of Arts degree in Forensic Psychology. Following my education, I graduated from the ATF's Special Agent Basic Training and from the Department of Homeland Security's Criminal Investigator Training Program. I have received training in the trafficking of firearms and controlled substances, as well as the various means and methods by which traffickers use in furtherance of firearms and narcotics transactions. I have also participated in multiple firearms and narcotics trafficking investigations involving the illegal sales, transfer, and possession of firearms and controlled substances. Additionally, I participated in many aspects of firearms and gang investigations, including conducting surveillance and the use of confidential informants and undercover agents to make controlled purchases of controlled substances and/or firearms.

III. SUMMARY OF PROBABLE CAUSE

6. On August 21, 2022, BPD patrol officers responded to a call for service regarding an individual who disposed of a duffel bag in a residential alleyway in Burbank, California. Inside of the black duffel bag, officers found a Kel-Tec, model PLR-16, 5.56 caliber pistol, bearing serial number P1101 along with thirteen rounds of .223 caliber ammunition. After obtaining witness statements and reviewing surveillance footage from a witness's home cameras, officers identified and arrested Sergio RUIZ ("RUIZ") who was walking nearby. Following RUIZ's arrest, the reporting individual identified him as the person who deposited the black duffel bag in the alleyway. The firearm and ammunition were all manufactured outside of the state of California. RUIZ is a convicted felon and domestic violence misdemeanor, and is, therefore, prohibited from possessing firearms or ammunition.

IV. STATEMENT OF PROBABLE CAUSE

7. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. BPD Patrol Officers Respond to a Call for Service

8. Based on my conversation with BPD Detective Ryan Benavidez and my review of the BPD report for this incident, I know that on August 21, 2022, at approximately 8:00 p.m., BPD Officers Lindquist, Bickel, and Campos responded to a call from BPD Dispatch regarding a male, later identified as RUIZ, who the reporting party saw dispose of a dark-colored duffel bag in a

residential alleyway in Burbank, California, specifically, at or near Lindon Court.

9. Based on my conversation with BPD Detective Ryan Benavidez and my review of the BPD report for this incident, I know that upon BPD officers' arrival at a residence near where RUIZ disposed of the duffel bag, the reporting party (N.I.) informed Officer Bickel where the duffel bag was located and stated that s/he had not gone near the duffel bag and did not know what was inside. At this time, Officers Bickel and Campos approached the duffel bag, looked inside, and saw a Kel-Tec, model PLR-16, 5.56 caliber pistol, bearing serial number P1101, inside the bag. Later, Officer Lindquist retrieved the firearm, and saw that the firearm was loaded and had an empty cartridge casing caught in the ejection port.

10. Officer Campos then spoke with a witness (J.H.), who resides near the location where the individual (later identified as RUIZ) disposed of the duffel bag. According to Officer Campos's report, J.H. told Officer Campos that s/he had video surveillance cameras on the outside of his/her residence.

11. J.H. showed Officer Campos the video from his/her surveillance cameras. According to Officers Campos's report, J.H.'s video surveillance captured a Hispanic male, wearing a light blue shirt, dark jeans, white shoes, and a white hat, walking in the residential alleyway, who dropped a duffel bag, later identified as the duffel bag containing the firearm. In the video, the man carried the duffel bag in his right hand and a cellphone in his left hand. The male set the duffel bag on

the ground, then turned around and walked away from it. The surveillance video was timestamped at approximately 7:59 p.m. on August 21, 2022. Officer Campos then broadcasted RUIZ's description over the radio.

12. While checking the area, BPD Officers Garner and Maus saw RUIZ approximately half a mile from the location where the duffel bag was found, at the intersection of Western Avenue and Lake Street in Glendale, California, and detained him. At the time, RUIZ was wearing the same clothes as the individual on the home surveillance footage: a light blue shirt, dark jeans, white shoes, and a white hat.

13. Shortly thereafter, Officer Campos read the witness, N.I., the Admonition for Field Identification of Suspects and then transported him/her where RUIZ was located. N.I. positively identified RUIZ as the male who dropped the duffel bag containing the gun in the alleyway and stated s/he was 100% positive it was RUIZ. Officers Camarena and Gorman then placed RUIZ under arrest and transported him to BPD jail for booking.

14. BPD officers recovered the SUBJECT DEVICE from RUIZ's person, during a search incident to arrest, at the time he was detained.

B. RUIZ's Mirandized Statements

15. Based on my review of a BPD supplemental report, I know the following:

a. BPD Officers Camarena and Gorman interviewed RUIZ upon arrival at the BPD Jail Facility. Officer Camarena read RUIZ his Miranda rights, which RUIZ stated he understood.

During the interview, RUIZ stated that he did not know why he was arrested by BPD because he was just out walking his dog. (RUIZ was not with a dog when he was arrested.) RUIZ also stated that he did not know anything about a duffel bag or what was inside the duffel bag.

b. While RUIZ was housed in a temporary holding cell, Officers Camarena and Gorman interviewed RUIZ a second time. RUIZ was not given a second Miranda warning prior to this interview. Officer Camarena played the surveillance footage obtained from witness J.H.'s home surveillance cameras, and asked RUIZ if he was the individual in the video. RUIZ replied, "I'm not saying it is or it's not." RUIZ later asked Officer Camarena why he was being asked so many questions and stated that he has rights and no longer wanted to answer any questions.

C. Criminal History

16. Based on my review of conviction documents and a rap sheet for RUIZ, I know that RUIZ has previously been convicted of the following felony crimes punishable by a term of imprisonment exceeding one year:

a. Possession of a Dangerous Weapon for Sale, in violation of California Penal Code Section 12020, in the Superior Court of the State of California, County of Los Angeles, case number NA027197, on or about May 30, 1996;

b. Felon in Possession of a Firearm, in violation of California Penal Code Section 12021(a)(1), in the Superior Court of the State of California, County of Los Angeles, case number NA045053, on or about September 7, 2000;

c. Assault with a Deadly Weapon on a Person Causing Great Bodily Injury, in violation of California Penal Code Section 245(a)(2), in the Superior Court of the State of California, County of Los Angeles, case number NA063187, on or about July 28, 2005; and

d. Bringing a Controlled Substance into a Prison, in violation of California Penal Code Section 4573, in the Superior Court of the State of California, County of Riverside, case number RIF500099, on or about April 21, 2015.

17. Furthermore, defendant RUIZ possessed such firearm and ammunition knowing that he had previously been convicted of a misdemeanor crime of domestic violence, namely, Domestic Battery, in violation of California Penal Code Section 243(e)(1), in the Superior Court for the State of California, County of Orange, case number 03WM07556, on or about September 26, 2003.

D. Interstate Nexus

18. On August 28, 2022, ATF Interstate Nexus Expert Bryan Traverso examined the firearm found in the duffel bag and determined it was a Kel-Tec Model PLR-16 5.56mm pistol, bearing serial number P1101. Special Agent Traverso also determined the firearm was manufactured in Florida. Because the handgun was found in California, I believe that it has traveled in and affected interstate commerce.

19. On the same date, Special Agent Traverso also examined thirteen rounds of ammunition found in the duffel bag. Of the thirteen rounds of ammunition, seven rounds were manufactured in

Missouri, four rounds were manufactured in the Philippines, and two rounds were manufactured in Israel. Because all thirteen rounds of ammunition were found in California, I believe they have traveled in and affected interstate and/or foreign commerce.

V. TRAINING AND EXPERIENCE ON FIREARMS OFFENSES

20. From my training, personal experience, and the collective experiences related to me by other law enforcement officers who conduct who conduct firearms investigations, I am aware of the following:

a. Persons who possess, purchase, or sell firearms generally maintain records of their firearm transactions as items of value and usually keep them in their residence, or in places that are readily accessible, and under their physical control, such in their digital devices. It has been my experience that prohibited individuals who own firearms illegally will keep the contact information of the individual who is supplying firearms to prohibited individuals or other individuals involved in criminal activities for future purchases or referrals. Such information is also kept on digital devices.

b. Many people also keep mementos of their firearms, including digital photographs or recordings of themselves possessing or using firearms on their digital devices. These photographs and recordings are often shared via social media, text messages, and over text messaging applications.

c. Those who illegally possess firearms often sell their firearms and purchase firearms. Correspondence between

persons buying and selling firearms often occurs over phone calls, e-mail, text message, and social media message to and from smartphones, laptops, or other digital devices. This includes sending photos of the firearm between the seller and the buyer, as well as negotiation of price. In my experience, individuals who engage in street sales of firearms frequently use phone calls, e-mail, and text messages to communicate with each other regarding firearms that they sell or offer for sale. In addition, it is common for individuals engaging in the unlawful sale of firearms to have photographs of firearms they or other individuals working with them possess on their cellular phones and other digital devices as they frequently send these photos to each other to boast of their firearms possession and/or to facilitate sales or transfers of firearms.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

21. As used herein, the term "digital device" includes the SUBJECT DEVICE.

22. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur

after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain

"booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

23. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

24. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally

displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. The person who is in possession of a device or has the device among his or her belongings is likely a user of the device. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress RUIZ's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of RUIZ's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

25. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. CONCLUSION

26. For all of the reasons described above, there is probable cause to believe that the items to be seized described in Attachment B will be found in a search of the SUBJECT DEVICE described in Attachment A

Attested to by the applicant in
accordance with the requirements
of Fed. R. Crim. P. 4.1 by
telephone on this ____ day of
September, 2022.

THE HONORABLE ROZELLA A. OLIVER
UNITED STATES MAGISTRATE JUDGE